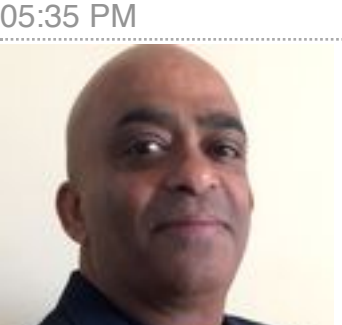
DARKReading

11/21/2019
05:35 PM



Jai Vijayan
News

Leaks of NSA, CIA Tools Have Leveled Nation-State Cybercriminal Capabilities

The wide availability of tools leaked by the Shadow Brokers and WikiLeaks in 2016 and 2017 have given emerging cyber powers a way to catch up, DarkOwl says.

The public leaks of classified NSA and CIA hacking tools in 2016 and 2017 appear to have leveled the playing field for nation-state cybercriminals to some extent, new research shows.

Threat intelligence firm DarkOwl recently analyzed Dark Web data gathered from public and proprietary sources and found the leaked cyber weapons have strengthened the ability of emerging nation-state actors to attack rivals and project attribution to others.

The NSA and CIA data — released publicly by a group called the Shadow Brokers and WikiLeaks, respectively — included an NSA espionage and mass-surveillance system called UNITEDRAKE, a multiplatform CIA malware suite called HIVE, and numerous documents describing sophisticated false-flag and other cyber-offense tactics.

The leaked cyber weapons have given adversaries new ways to capture text, video, and images from target systems, including the Internet of Things (IoT) and smart TVs; attack smart vehicles; hide implants in Windows and other operating systems; and conduct a range of other surreptitious actions. Significantly, the leaks also made widely available capabilities that let attackers conceal the origins of an attack or to make it appear as if an attack originated from somewhere else entirely.

Details on the NSA and CIA tools and processes have been extensively studied on the Dark Web and

are now part of the arsenal of everyone from nation-state actors to ordinary cybercriminals, DarkOwl says. "The wide dissemination of cyber weapons from the NSA and CIA has changed the international cyber battle space considerably," says Andrew Lewman, vice president at DarkOwl. "Sophisticated, weapons-grade cyber tools are available on the Dark Web and [are creating] numerous challenges in determining who could be behind various cyber campaigns."

The US, Russia, and China continue to be cyber superpowers in terms of skills, influence, money, and manpower. But other less powerful nations have acquired formidable strength because of their access to these previously unattainable tools. "At this time, we do not have enough intelligence to support a statement on what country has benefited the most from the leaks of these tools," Lewman says. But a generalized leveling of the playing field since the NSA and CIA leaks is clear, he notes.

In DarkOwl's assessment, Israel, Germany, and the UK rank behind the top three nations in their cyber capabilities, followed by Ukraine, France, Iran, and India. But it is Iran and North Korea that present a major threat to US interests in cyberspace, especially given their ongoing cooperation and collaboration in military and technology development, Lewman says.

Cyber proxies, specifically as contracted by the Kingdom of Saudi Arabia, are another increasing concern because previously the Kingdom displayed little to no cyber capabilities. "Financial resources and international influence is of concern for them and their role in international conflicts," Lewman says.

Leveraging the Dark Web

DarkOwl's research shows that nation-state funded threat groups are leveraging the Dark Web in multiple ways. One of the most common is for infrastructure disruption campaigns targeted at networks containing sensitive government or corporate information. Many are using the cover of the Dark Web — and tools from the NSA and CIA leaks — to go after critical infrastructure targets, as well.

Attacks earlier this year involving the use of Triton malware against Triconex industrial-control systems are one example, Lewman says. Triton — a tool the NSA has previously used — is designed specifically to exploit weaknesses in industry control systems.

The Dark Web also has been a source of credentials and other information for state-backed threat groups seeking to break into the networks of governments they perceive as being hostile or being of geopolitical or military interest.

"For example, the Dark Web is replete with US *.gov email addresses that could be exploited for brute-force network intrusion or targeted phishing campaigns," DarkOwl said. According to the vendor, there were over a half-million Dark Web pages with credentials that included a .gov address.

"Nation-state actors, cyber proxies, and terrorists will continue to use the Dark Web for operations, albeit not in as straightforward means as we'd assume," Lewman says.

Related Content:

- Shadow Brokers Offers Database Of Windows Exploits For Sale
- 'Entire Hacking Capacity Of CIA' Dumped On Wikileaks, Site Claims
- Triton/Trisis Attack Was More Widespread Than Publicly Known
- What You Need to Know About Zero Trust Security

Check out The Edge, Dark Reading's new section for features, threat data, and in-depth perspectives. Today's top story: "What's in a WAF?"

Jai Vijayan is a seasoned technology reporter with over 20 years of experience in IT trade journalism. He was most recently a Senior Editor at Computerworld, where he covered information security and data privacy issues for the publication. Over the course of his 20-year ... View Full Bio